

03/28/00  
U.S. PTO

03-24-00

A

Express Mail Label No. EL521605828US

# UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.  
11345/009001

Total Pages in this Submission

## TO THE ASSISTANT COMMISSIONER FOR PATENTS

Box Patent Application  
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM TRANSMISSION

and invented by:

Michael MAILLARD, Christian BENARDEAU, Jean-Luc DAUVOIS

JC586 U.S. PTO  
09/537071  
03/28/00

If a **CONTINUATION APPLICATION**, check appropriate box and supply the requisite information:

☒ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: PCT/IB98/01610

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: \_\_\_\_\_

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: \_\_\_\_\_

Enclosed are:

### Application Elements

1. ☐ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 24 pages and including the following:
  - a. ☒ Descriptive Title of the Invention
  - b. ☐ Cross References to Related Applications (if applicable)
  - c. ☐ Statement Regarding Federally-sponsored Research/Development (if applicable)
  - d. ☐ Reference to Microfiche Appendix (if applicable)
  - e. ☒ Background of the Invention
  - f. ☒ Brief Summary of the Invention
  - g. ☒ Brief Description of the Drawings (if drawings filed)
  - h. ☒ Detailed Description
  - i. ☒ Claim(s) as Classified Below
  - j. ☒ Abstract of the Disclosure



22511

PATENT TRADEMARK OFFICE

# UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.  
11345/009001

Total Pages in this Submission

## Application Elements (Continued)

3. ☒ Drawing(s) (when necessary as prescribed by 35 USC 113)
- a. ☒ Formal                      Number of Sheets 5
- b. ☐ Informal                      Number of Sheets \_\_\_\_\_
4. ☒ Oath or Declaration
- a. ☒ Newly executed (original or copy)      ☐ Unexecuted
- b. ☐ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional application only)
- c. ☒ With Power of Attorney      ☐ Without Power of Attorney
- d. ☐ DELETION OF INVENTOR(S)  
Signed statement attached deleting inventor(s) named in the prior application,  
see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference (usable if Box 4b is checked)  
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Computer Program in Microfiche (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all must be included)
- a. ☐ Paper Copy
- b. ☐ Computer Readable Copy (identical to computer copy)
- c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

## Accompanying Application Parts

8. ☒ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(B) Statement (when there is an assignee)
10. ☐ English Translation Document (if applicable)
11. ☒ Information Disclosure Statement/PTO-1449      ☒ Copies of IDS Citations
12. ☒ Preliminary Amendment
13. ☒ Acknowledgment postcard
14. ☒ Certificate of Mailing

☐ First Class      ☒ Express Mail (Specify Label No.): EL521605828US

**UTILITY PATENT APPLICATION TRANSMITTAL**  
**(Large Entity)**

*(Only for new nonprovisional applications under 37 CFR 1.53(b))*

Docket No.  
11345/009001

Total Pages in this Submission

**Accompanying Application Parts (Continued)**

15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. ☒ Additional Enclosures *(please identify below):*

IPEA Report for PCT/IB98/01610 dated December 30, 1999 (6 pgs.)  
PCT Search Report for PCT/IB98/01610 dated April 12, 1998 (10 pgs.)  
PCT Written Opinion for PCT/IB98/01610 dated July 7, 1999 (8 pgs.)  
Response to PCT Written Opinion for PCT/IV98/01610 dated November 22, 1999 (3 pgs.)

**Fee Calculation and Transmittal**

**CLAIMS AS FILED**

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	22	- 20 =	2	x \$18.00	\$36.00
Indep. Claims	2	- 3 =	0	x \$78.00	\$0.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
BASIC FEE					\$690.00
OTHER FEE (specify purpose) Assignment fee					\$40.00
TOTAL FILING FEE					\$766.00

- ☒ A check in the amount of \$766.00 to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. 500-591 as described below. A duplicate copy of this sheet is enclosed.
- ☐ Charge the amount of \_\_\_\_\_ as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

*Jonathan P. Osha* Reg. No. 33,986 for  
Signature

Jonathan P. Osha  
Reg. No. 33,986  
ROSENTHAL & OSHA L.L.P.  
700 Louisiana, Suite 4550  
Houston, Texas 77002

Dated:

CC:

Telephone: (713) 228-8600  
Facsimile: (713) 228-8778

**CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)**

Applicant(s): Michel MAILLARD et al.

Docket No.

11345/009001

Serial No.

Filing Date

Examiner

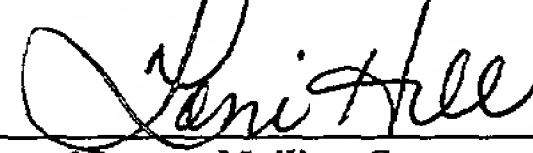
Group Art Unit

Invention: **METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM TRANSMISSION**

JC586 U.S. PTO  
09/537071  
03/28/00

I hereby certify that this Assignment*(Identify type of correspondence)*

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under  
37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on  
March 29, 2000

*(Date)*Toni Hill*(Typed or Printed Name of Person Mailing Correspondence)**(Signature of Person Mailing Correspondence)*EL521605828US*("Express Mail" Mailing Label Number)***Note: Each paper must have its own certificate of mailing.**

**CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)**Applicant(s): **Michel MAILLARD et al.**

Docket No.

**11345/009001**

Serial No.

Filing Date

Examiner

Group Art Unit

Invention: **METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM TRANSMISSION**

jc685 U.S. PTO

09/537071



03/28/00

I hereby certify that this **Preliminary Amendment***(Identify type of correspondence)*

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under  
37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on  
**March 29, 2000**

*(Date)***Toni Hill***(Typed or Printed Name of Person Mailing Correspondence)**(Signature of Person Mailing Correspondence)***EL521605828US***("Express Mail" Mailing Label Number)***Note: Each paper must have its own certificate of mailing.**

**CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)**Applicant(s): **Michel MAILLARD et al.**

Docket No.

**11345/009001**

Serial No.

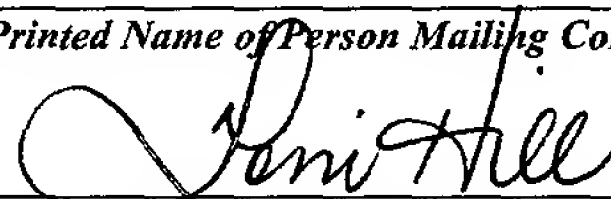
Filing Date

Examiner

Group Art Unit

Invention: **METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM TRANSMISSION**JC586 U.S. PTO  
09/537071  
03/28/00I hereby certify that this **Rule 371 Continuation Patent Application***(Identify type of correspondence)*

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under  
37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on  
**March 28, 2000**

*(Date)***Toni Hill***(Typed or Printed Name of Person Mailing Correspondence)**(Signature of Person Mailing Correspondence)***EL521605828US***("Express Mail" Mailing Label Number)***Note: Each paper must have its own certificate of mailing.****EL521605828US**

**CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)**

Applicant(s): Michel MAILLARD et al.

Docket No.

11345/009001

Serial No.

Filing Date

Examiner

Group Art Unit

Invention: METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM TRANSMISSION

JC586 U.S. PTO

09/537071



03/28/00

I hereby certify that this Information Disclosure Statement*(Identify type of correspondence)*

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under  
37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on  
March 29, 2000

*(Date)*Toni Hill*(Typed or Printed Name of Person Mailing Correspondence)**(Signature of Person Mailing Correspondence)*EL521605828US*("Express Mail" Mailing Label Number)***Note: Each paper must have its own certificate of mailing.**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Michael MAILLARD et al. Art Unit:  
Serial No.: Examiner:  
Filed: Herewith  
Title: METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM  
TRANSMISSION

jc685 U.S. PTO  
09/537071  
03/28/00

Box Patent Application  
Assistant Commissioner for Patents  
Washington, DC 20231



22511

PATENT TRADEMARK OFFICE

**PRELIMINARY AMENDMENT**

Dear Sir:

Before examining the referenced application on the merits, please amend the application as outlined below:

**In the Specification:**

On Page 1, line 1, please insert the phrase --This is a continuation of International Application PCT/IB98/01610, with an international filing date of October 2, 1998.-- before the word "The".

**In the Claims:**

In claim 2, line 1, please delete "1" and replace with --24--.

In claim 4, line 3, please delete "decoder" and replace with --security module--.

In claim 11, line 1, please delete "or 10".

In claim 12, line 1, please delete "any of claims 7 to 11" and replace with --7--.

In claim 14, line 1, please delete "1" and replace with --24--.



In claim 17, line 1, please delete "any of claims 14 to 16" and replace with --14--.

In claim 19, line 1, please delete "any of claims 1 to 18" and replace with --24--.

In claim 20, line 1, please delete "any of claims 1 to 18" and replace with --24--.

In claim 21, line 1, please delete "any preceding claim" and replace with --24--.

Please cancel claims 1, 18, 22 and 23 and add the following new claims:

--24. A method of transmission and reception of a scrambled data stream

comprising:

transmitting a scrambled data stream to a decoder;

sending the scrambled data stream to a portable security module inserted in the  
decoder;

descrambling the scrambled data stream;

encrypting a descrambled data stream;

sending the encrypted data stream to the decoder;

decrypting the encrypted data stream; and

using the decrypted data stream.

25. A method of transmission and reception of scrambled data as claimed in  
claim 2, further comprising:

encrypting the data stream at the point of transmission by a first encryption key;

and

decrypting the data stream by the decoder by an equivalent of the first encryption  
key.

26. An apparatus for the transmission and reception of a scrambled data stream comprising:
- a decoder; and
  - a portable security module.--

**REMARKS**

The claims have been amended to remove multiple dependencies and to correct antecedent basis errors. Full examination and favorable action are requested.

Please charge any fees, or make any credits, to Deposit Account No. 500-591, Reference No. 11345/009001.

Date: 3/28/00

Richard A. Fagin reg no 39,182  
Jonathan P. Osha  
Reg. No. 33,986

Rosenthal & Osha L.L.P.  
700 Louisiana Street, Suite 4550  
Houston, TX 77002

Telephone: 713/228-8600  
Facsimile: 713/6228-8778

11345.006001.200003017.01.doc

**APPLICATION**  
**FOR**  
**UNITED STATES LETTERS PATENT**

JC685 U.S. PTO  
09/537071  
03/28/00

**TITLE:** **METHOD AND APPARATUS FOR ENCRYPTED  
DATA STREAM TRANSMISSION**

**APPLICANT:** **Michel MAILLARD, Christian BENARDEAU,  
Jean-Luc DAUVOIS**

**"EXPRESS MAIL" Label No.:** EL521605828US

**Date of Deposit:** March 28, 2000



**22511**

PATENT TRADEMARK OFFICE

-1-

**METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM**  
**TRANSMISSION**

5 The present invention relates to a method and apparatus for use with an encrypted or scrambled transmission, for example a scrambled television broadcast.

10 Transmission of encrypted data is well-known in the field of pay TV systems, where scrambled audiovisual information is usually broadcast by satellite to a number of subscribers, each subscriber possessing a decoder or receiver/decoder capable of descrambling the transmitted program for subsequent viewing.

15 In a typical system, scrambled data is transmitted together with a control word for descrambling of the data, the control word itself being encrypted by a so-called exploitation key and transmitted in encrypted form. The scrambled data and encrypted control word are then received by a decoder having access to an equivalent of the exploitation key stored on a smart card inserted in the decoder to decrypt the encrypted control word and thereafter descramble the transmitted data. A paid-up subscriber will receive in a monthly ECM (Entitlement Control Message) the exploitation key necessary to decrypt the encrypted control word so as to permit  
20 viewing of the transmission.

25 In order to try to improve the security of the system, the control word is usually changed every ten seconds or so. This avoids the situation with a static or slowly changing control word where the control word may become publicly known. In such circumstances, it would be relatively simple for a fraudulent user to feed the known control word to the descrambling unit on his decoder to descramble the transmission.

30 Notwithstanding this security measure, a problem has arisen in recent years where the stream of control words sent during a broadcast film, for example, becomes known. This information may be used by any unauthorised user who has recorded the still-scrambled film on a video recorder. If the film is replayed at the same time as the stream of control words is fed to the decoder, visualisation of the film becomes

-2-

possible. Provided the user manages to synchronise the film with the control stream there are no great technical problems in carrying out such a fraud, particularly since the hardware elements necessary to build the descrambler are easily obtained.

- 5 This problem has been exacerbated with the rise of the internet and it is now not uncommon to find any number of internet sites that publish the stream of control words emitted during a given transmission.

10 It is an object of the present invention to overcome the problems associated with known prior art techniques for scrambled transmissions so as to provide a secure decoder configuration resistant to attacks such as those described above.

15 According to the present invention there is provided a method of transmission and reception of a scrambled data stream in which the scrambled data stream is transmitted to a decoder, and thereafter passed to and descrambled by a portable security module inserted in the decoder and characterised in that the data stream is passed from the security module to the decoder in an encrypted form, to be decrypted and subsequently used by the decoder.

20 As discussed above, in conventional systems, a control word is encrypted by an exploitation key and passed from the decoder to the smart card for decryption before being passed in a decrypted form to the control unit in the decoder for descrambling of the transmission. The weak point in such techniques lies in the transmission of the control word "in clear" between the card and the decoder unit, since it is relatively  
25 easy to determine the connections between the card and the decoder and to thereafter record the control word information passing along these connections.

By identifying this weakness, and proposing a solution in which data is descrambled by a portable security module before being passed back to the decoder in an encrypted  
30 form the present invention overcomes the problems with these techniques.

According to a first type of realisation of the invention, the data stream is encrypted

-3-

in the security module by a first encryption key before being passed back to the decoder for decryption using an equivalent of the first key. However, as will be described below, other realisations of the invention are possible, in which the data is passed from security module to decoder in encrypted form but in which the encryption takes place at the transmission level.

In one embodiment of the above realisation, the data stream is encrypted in the security module by a first encryption key variable in dependence on a decoder identity value, the decoder possessing an equivalent of the key and value necessary to decrypt the data. For example, the decoder identity value can correspond to the serial or batch number of the decoder.

The decoder identity value may be encrypted by a personalised key known to the security module and transmitter, the decoder identity value being transmitted in an encrypted form to the decoder for communication to the security module. Once decrypted by the personalised key within the security module the decoder identity value and first encryption key can be used by the security module to create the encrypted data stream.

Communication of the decoder identity value to the security module will necessarily involve a signal being sent from the decoder to the security module. As we have seen, the transmission of messages across this channel is relatively easy to monitor and it is thus preferable to transfer the identity value in a non-readable form to the security module.

Personalised keys of this type are known in relation to EMMs or Entitlement Management Messages, which transmit each month in encrypted form a management key for decrypting that month's ECM to a selected subscriber or group of subscribers possessing the necessary personalised key to decrypt the EMM.

In an another solution, the decoder identity value may be encrypted by a personalised key known to the security module, the encrypted decoder identity value being stored

-4-

in the decoder during manufacture of the decoder for communication to the security module upon insertion of the security module in the decoder.

5 In an alternative to the use of a fixed decoder identity value, the first encryption key may be dependent on a random or pseudo-random number generated, for example, by the decoder and communicated to the security module.

10 Preferably, and in view of the problems associated in communicating non-encrypted data between the decoder and the security module, the random number is encrypted by a second encryption key before being communicated between the decoder and security module, or vice versa.

15 In one embodiment, the random number may be generated and encrypted by a second encryption key at the decoder and communicated to the security module for decryption by an equivalent of this second key stored in the security module.

20 In an alternative embodiment, the operation of the security module and decoder may simply be reversed, such that the random number is generated and encrypted by a second key in the security module and communicated to the decoder for decryption by an equivalent of the second key stored in the decoder.

25 In the examples given above, the first and second encryption key, the personalised security module key etc may all be created in accordance with a known symmetric encryption algorithm, such as DES, RC2 etc. However, in a preferred embodiment where the decoder is responsible for generation of the random number, the second key used to encrypt the random number corresponds to a public key, the security module being provided with the equivalent private key necessary to decrypt the random number value.

30 As compared with a portable security module such as a smart card, the hardware component in the decoder used to store the first and second encryption keys (typically a ROM) is relatively easy to isolate and monitor by means of attached contacts etc.



A dedicated fraudulent user may therefore obtain the first and second keys and, by monitoring communications between the security module and decoder, the encrypted value of the random number. If a symmetric algorithm is used for the second key, the random number may then be decrypted with the known decoder second key and fed  
5 to the known first key to decrypt the control word.

In contrast, through the use of a public key/private key arrangement, possession of the second public key held by the decoder does not enable a fraudulent user to decode the encrypted random number. Whilst it is always possible to obtain the random number  
10 directly, this is more difficult in comparison with obtaining the keys and picking up the communicated encrypted value, since the random number will be most likely generated and stored somewhere in the RAM of the decoder and can in any case change on a regular basis.

15 Preferably, the second private key is unique to the security module. This embodiment substantially increases the security of the system, although as will be understood the data stream communicated between the security module and decoder will be in any case dependent on the random number generated during that session.

20 As mentioned above, the use of a public/private key arrangement in relation to the second encryption key is particularly advantageous where the private key is stored in the security module and the public key in the decoder. However, in alternative embodiments, the situation may be reversed such that the private key is held in the decoder and the public key in the security module.

25 Advantageously, the second decoder key is encrypted by a third key before communication to the decoder, the decoder possessing the corresponding third key so as to decrypt and verify the second decoder key.

30 In a particularly advantageous embodiment, the third key used to decrypt the second decoder key is a private key, the decoder possessing the equivalent public key to decrypt and verify the communicated second key.



-6-

In all of the above embodiments of this first type of realisation, the data stream is re-encrypted by a first encryption key held in the security module before being passed to the decoder.

5 As mentioned, in an alternative type of realisation, the encrypted data stream passed between the security module and decoder is prepared upstream of the security module. In such realisations, the data stream is encrypted at the point of transmission by a first encryption key and decrypted by the decoder by an equivalent of this key.

10 In a preferred embodiment, the data stream is encrypted at the point of transmission by a first encryption key dependant on a variable known to both the transmitter and the decoder and decrypted by the decoder by an equivalent of this key and variable.

15 For example, the data stream may be encrypted at the point of transmission by a first encryption key dependant on the real time and/or date of transmission. In such a case, the encrypted data stream will only function at the time of transmission of the broadcast and cannot be fed into the descrambler of a decoder after the broadcast has been recorded since the decryption key of the decoder (or rather its associated variable) will now have changed.

20

As will be appreciated, whilst this realisation is less secure than the embodiments of first realisation discussed above, it possesses the advantage that no changes to the hardware of existing security modules are necessary. Furthermore, the modifications to the decoder and transmitter needed to implement the invention can be implemented  
25 in software, e.g. in the case of the decoder by the downloading of transmitted data.

In this second type of realisation, the encrypted data stream can be further encrypted by an exploitation key at the point of transmission, decrypted by an equivalent exploitation key in the security module and then passed in its first encrypted form to  
30 the decoder.

As described in all the above embodiments, the data stream passed in encrypted form

-7-

between the security module and decoder may comprise audiovisual data. In such an embodiment, after decryption of the data stream, the decoder will simply display the audio visual data.

5 However, in an alternative embodiment, the data stream passed in encrypted form between the security module and decoder may comprise a control word stream, the decrypted control word stream being used thereafter by the decoder to descramble associated scrambled audiovisual data.

10 In such an embodiment, the " scrambling " and " descrambling " of the control word data stream as described above corresponds to the encryption and decryption of ECM messages using an exploitation key, as in conventional systems.

15 In order to increase the security of the system, any or all of the above described embodiments may implemented in combination with each other.

The present invention is particularly applicable to the transmission of a television broadcast. The present invention also extends to a decoder and security module adapted for a method of transmission as described above.

20

The term "portable security module" is used to mean any conventional chip-based portable card type devices possessing, for example, microprocessor and/or memory storage. This may include smart cards, PCMCIA cards, SIM cards etc. Included in this term are chip devices having alternative physical forms, for example key-shaped devices such as are often used in TV decoder systems.

25

The terms " scrambled " and " encrypted " and " control word " and " key " have been used here in a number of ways for the purpose of clarity of language. However, it will be understood that no fundamental distinction is to be made between  
30 " scrambled data " and " encrypted data " or between a " control word " and a " key ".

Similarly, whilst the description refers to " receiver/decoders " and " decoders " it will be understood that the present invention applies equally to embodiments having a receiver integrated with the decoder as to a decoder unit functioning in combination with a physically separate receiver, decoder units incorporating other functionalities, and decoder units integrated with other devices, such as televisions, recording devices etc.

A number of embodiments of the invention will now be described by way of example only and in relation to the attached figures, in which:

10

Figure 1 shows the overall architecture of a known digital television system, as may be adapted by the present invention;

15

Figure 2 shows the conditional access system of the television system of Figure 1;

Figure 3 shows a first embodiment of the invention;

Figure 4 shows a second embodiment of the invention; and

20

Figure 5 shows a third embodiment of the invention.

### Digital Television System

An overview of a digital television broadcast and reception system 1000 adaptable to the present invention is shown in Figure 1. The system includes a mostly conventional digital television system 2000, which uses the known MPEG-2 compression system to transmit compressed digital signals. In more detail, the MPEG-2 compressor 2002 in a broadcast centre receives a digital signal stream (typically a stream of video signals). The compressor 2002 is connected to a multiplexer and scrambler 2004 by linkage 2006. The multiplexer 2004 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 2008 of the broadcast centre via linkage 2010, which can of course take

-9-

a wide variety of forms including telecom links. The transmitter 2008 transmits electromagnetic signals via uplink 2012 towards a satellite transponder 2014, where they are electronically processed and broadcast via notional downlink 2016 to earth receiver 2018, conventionally in the form of a dish owned or rented by the end user.

5 The signals received by receiver 2018 are transmitted to an integrated receiver/decoder 2020 owned or rented by the end user and connected to the end user's television 2022. The receiver/decoder 2020 decodes the compressed MPEG-2 signal into a television signal for the television set 2022.

10 A conditional access system 3000 is connected to the multiplexer 2004 and the receiver/decoder 2020, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smart card, capable of decrypting messages relating to commercial offers (that is, on or several television programmes sold by the broadcast  
15 supplier), can be inserted into the receiver/decoder 2020. Using the decoder 2020 and smart card, the end user may purchase events in either a subscription mode or a pay-per-view-mode.

20 An interactive system 4000, also connected to the multiplexer 2004 and the receiver/decoder 2020 and again located partly in the broadcast and partly in the decoder, enables the end user to interact with various applications via a modemmed back channel 4002.

#### Conditional Access System

25

With reference to Figure 2, the conditional access system 3000 includes a Subscriber Authorization System (SAS) 3002. The SAS 3002 is connected to one or more Subscriber Management Systems (SMS) 3004, one SMS for each broadcast supplier, by a respective TCP-IP link 3006 (although other types of linkage could alternatively  
30 be used). Alternatively, one SMS could be shared between two broadcast suppliers, or one supplier could use two SMSs, and so on.

-10-

First encrypting units in the form of ciphering units 3008 utilising "mother" smart cards 3010 are connected to the SAS by linkage 3012. Second encrypting units again in the form of ciphering units 3014 utilising mother smart cards 3016 are connected to the mutliplexer 2004 by linkage 3018. The receiver/decoder 2020 receives a  
5 "daughter" smart card 3020. It is connected directly to the SAS 3002 by Communications Servers 3022 via the modemmed back channel 4002. The SAS sends amongst other things subscription rights to the daughter smart card on request.

The smart cards contain the secrets of one or more commercial operators. The  
10 "mother" smart card encrypts different kinds of messages and the "daughter" smart cards decrypt the messages, if they have the rights to do so.

The first and second ciphering units 3008 and 3014 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one  
15 smart card 3010 and 3016 respectively, for each electronic card, one (card 3016) for encrypting the ECMs and one (card 3010) for encrypting the EMMS.

#### Multiplexer and Scrambler

20 With reference to Figures 1 and 2, in the broadcast centre, the digital video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 2002. This compressed signal is then transmitted to the multiplexer and scrambler 2004 via the linkage 2006 in order to be multiplexed with other data, such as other compressed data.

25

The scrambler generates a control word CW used in the scrambling process and included in the MPEG-2 stream in the multiplexer 2004. The control word CW is generated internally and enables the end user's integrated receiver/decoder 2020 to descramble the programme. Access criteria, indicating how the programme is  
30 commercialised, are also added to the MPEG-2 stream. The programme may be commercialised in either one of a number of "subscription" modes and/or one of a number of "Pay Per View" (PPV) modes or events. In the subscription mode, the

end user subscribes to one or more commercial offers, of "bouquets", thus getting the rights to watch every channel inside those bouquets. In the preferred embodiment, up to 960 commercial offers may be selected from a bouquet of channels. In the Pay Per View mode, the end user is provided with the capability to purchase events as he wishes. This can be achieved by either pre-booking the event in advance ("pre-book mode"), or by purchasing the event as soon as it is broadcast ("impulse mode").

Both the control word CW and the access criteria are used to build an Entitlement Control Message (ECM); this is a message sent in relation with one scrambled program. The message contains a control word (which allows for the descrambling of the program) and the access criteria of the broadcast program. The access criteria and control word are transmitted to the second encrypting unit 3014 via the linkage 3018. In this unit an ECM is generated, encrypted with an exploitation key Cex and transmitted on to the multiplexer and scrambler 2004.

#### Programme Transmission

The multiplexer 2004 receives electrical signals comprising encrypted EMMs from the SAS 3002, encrypted ECMs from the second encrypting unit 3014 and compressed programmes from the compressor 2002. The multiplexer 2004 scrambles the programmes and transmits the scrambled programmes, the encrypted EMM (if present) and the encrypted ECMs as electric signals to a transmitter 2008 of the broadcast centre via linkage 2010. The transmitter 2008 transmits electromagnetic signals towards the satellite transponder 2014 via uplink 2012.

#### Programme Reception

The satellite transponder 2014 receives and processes the electromagnetic signals transmitted by the transmitter 2008 and transmits the signals on to the earth receiver 2018, conventionally in the form of a dish owned or rented by the end user, via downlink 2016. The signals received by receiver 2018 are transmitted to the integrated receiver/decoder 2020 owned or rented by the end user and connected to the end



-12-

user's television set 2022. The receiver/decoder 2020 demultiplexes the signals to obtain scrambled programmes with encrypted EMMs and encrypted ECMs.

If the programme is not scrambled the receiver/decoder 2020 decompresses the data and transforms the signal into a video signal for transmission to television set 2022.

If the programme is scrambled, the receiver/decoder 2020 extracts the corresponding ECM from the MPEG-2 stream and passes the ECM to the "daughter" smart card 3020 of the end user. This slots into a housing in the receiver/decoder 2020. The daughter smart card 3020 controls whether the end user has the right to decrypt the ECM and to access the programme. If not, a negative status is passed to the receiver/decoder 2020 to indicate that the programme cannot be descrambled. If the end user does have the rights, the ECM is decrypted and the control word extracted. The decoder 2020 can then descramble the programme using this control word. The MPEG-2 stream is decompressed and translated into a video signal onward transmission to television set 2022.

#### Subscriber Management System (SMS)

A Subscriber Management System (SMS) 3004 includes a database 3024 which manages, amongst others, all of the end user files, commercial offers (such as tariffs and promotions), subscriptions, PPV details, and data regarding end user consumption and authorization. The SMS may be physically remote from the SAS

Each SMS 3004 transmits messages to the SAS 3002 via respective linkage 3006 to enable modifications to or creations of Entitlement Management Messages (EMMs) to be transmitted to end users.

The SMS 3004 also transmits messages to the SAS 3002 which imply no modifications or creations of EMMs but imply only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).

Entitlement Management Messages and Entitlement Control Messages

- ECMs or Entitlement Control Messages are encrypted messages embedded in the data stream of a transmitted program and which contain the control word necessary for descrambling of a program. Authorisation of a given receiver/decoder is controlled by EMMs or Entitlement Management Messages, transmitted on a less frequent basis and which supply an authorised receiver/decoder with the exploitation key necessary to decode the ECM.
- 10 An EMM is a message dedicated to an individual end user (subscriber), or a group of end users. A group may contain a given number of end users. This organisation as a group aims at optimising the bandwidth; that is, access to one group can permit the reaching of a great number of end users.
- 15 Various specific types of EMM may be used. Individual EMMs are dedicated to individual subscribers, and are typically used in the provision of Pay Per View services. So-called " Group " subscription EMMs are dedicated to groups of, say, 256 individual users, and are typically used in the administration of some subscription services. This EMM has a group identifier and a subscribers' group bitmap
- 20 For security reasons, the control word CW embedded in an encrypted ECM changes on average every 10 seconds or so. In contrast, the exploitation key Cex used by the receiver to decode the ECM is changed every month or so by means of an EMM. The exploitation key Cex is encrypted using a personalised key corresponding to the
- 25 identity of the subscriber or group of subscribers recorded on the smart card. If the subscriber is one of those chosen to receive an updated exploitation key Cex, the card will decrypt the message using its personalised key to obtain that month's exploitation key Cex.
- 30 The operation of EMMs and ECMs will be well-known to one skilled in the art and will not be described here in any more detail.



Encryption of Data Stream by Smart Card

Referring now to Figures 3 and 4, a number of embodiments of a first realisation of the present invention will now be described. As shown in Figure 3, a scrambled  
5 audiovisual data stream is received by the receiver/decoder 3020 and passed to the portable security module 3020 where it is descrambled at 3030 using the exploitation key Cex possessed by the card to generate the decrypted control word CW and thereafter descramble the transmission. As will be understood, in this invention, the descrambling of a transmission is carried out entirely on the portable security module,  
10 which may comprise a smart card, a PCMCIA card etc.

Before being passed back to the decoder, the data stream is re-encrypted according to a first encryption key Kf at 3031. The operation of the key Kf is dependant on a decoder identity value N associated with the identity of the decoder, for example its  
15 serial number. This value N is communicated to the card by means of an encrypted EMM, transmitted at the initialisation of the decoder/card system and passed by the decoder 2020 to the card 3020 for decryption at the point 3032.

As with all EMM messages, the EMM containing the identity value N is encrypted  
20 by means of a personalisation key corresponding to a key held by the card and known by the transmitter of the message, which enables that card or group of cards to decode the encrypted EMM.

In an alternative embodiment, the initialising EMM can be pre-stocked in the memory  
25 of the decoder and sent to the card upon the first insertion of the card, or each time the decoder is turned on. In the latter case the card will be programmed to accept the initialising EMM only the first time that it receives it. Again, as with the transmitted EMM, the personalisation key associated with the card will be used to encrypt and decrypt the transmitted value.

30

Turning now to the decoder 2020, this is also provided with a key Kf and, of course, its identity or serial number N. The key Kf and number N may be stocked, for

-15-

example, in the ROM of the decoder. Using the key Kf and identity value N, the decoder decrypts the descrambled data stream. In practice the identity value need not be fixed, and it would be a simple matter to reprogram the identity value N stored within the card and decoder if this proved necessary.

5

In this embodiment, the key Kf can most simply be created using any known symmetric key algorithm for generating a key capable of being diversified by a given value (such as the identity value N in the above example). A public/private key pairing is also conceivable, the public key being associated with the decoder, the private key with the smart card. As in conventional systems, the exploitation key and personalisation key may be generated by a symmetric algorithm.

10

As will be understood, the data stream is only transmitted between the card and decoder in an encrypted or scrambled form, thereby reducing the risk of the type of fraud described in the introduction of the application. Furthermore, in this embodiment, all communications between the card and decoder are in fact encrypted, thereby increasing the security of the system.

15

In the above embodiment, the data stream decrypted at 3030 and re-encrypted at 3031 corresponds to a stream of audiovisual data. In an alternative embodiment, the data stream may correspond to a stream of control word data, decryption of ECMs being carried out at 3030 to generate a control word stream re-encrypted at 3031 and communicated to the decoder. The decrypted control word stream produced at 3033 by the decoder is thereafter used by the decoder to descramble scrambled audiovisual data transmitted and associated with the control word stream.

20

25

The advantage of such an embodiment is that the circuitry necessary to process and descramble the flow of audiovisual data is embodied within the decoder, rather than in the security module, which handles only the decryption and re-encryption of the control word stream.

30

One drawback of the system of Figure 3 lies in the fact that, although not trivial, the

extraction of the key  $K_f$  and identity value  $N$  from the ROM of the decoder may be carried out without too much difficulty. The embodiment of Figure 4 overcomes this weakness.

- 5 As shown, a random or pseudo-random number  $RN$  is generated within the decoder at 3040 and passed for subsequent encryption at 3041 by a public key  $K_{pub}$  of a suitable public/private key algorithm, such as RSA. The corresponding private key  $K_{pri}$  is held by the smart card. The encrypted random number  $p(RN)$  is then passed to the smart card which uses the private key  $K_{pri}$  to decrypt at 3042 the encrypted  
10 random number value  $p(RN)$ .

- As with the identity value  $N$  in the previous embodiment, the value  $RN$  is used at 3031 in the encryption by a symmetric key  $K_f$  of the descrambled data stream so as to obtain an encrypted data stream then passed from the card to the decoder. The  
15 communication of the original scrambled data stream from the decoder to the smart card has been omitted here in order to simplify the diagram.

- On the side of the decoder, the encrypted value data stream is decrypted at 3033 using the symmetric key  $K_f$  and the random number value  $RN$ . Unlike the identity value  
20  $N$  of the previous embodiment, the random number  $RN$  can be a frequently changing value stored in the RAM of the decoder and, as such, relatively difficult to identify. The public key  $K_{pub}$  and symmetric key values are stored in a more permanent fashion in the device and, as such, are less secure. However, even in the event that an unauthorised user manages to obtain these keys, and the encrypted value  $p(RN)$ ,  
25 it will not be possible to generate the  $RN$  value needed to decrypt the data stream from this information because of the nature of private/public key algorithms and the security of the control word will remain uncompromised.

- The same public/private key pair can be used for a series of decoders and cards.  
30 However, the level of security will be increased through the use of a unique public/private key pair associated with that smart card.

-17-

As shown, the values of Kpub and Kpri are generated by the system operator shown at 3050 and embedded in the smart card 3020. The value of Kpub will then be communicated to the decoder at the moment of insertion of the smart card in the decoder. Since the public key Kpub will be used to encrypt the random number RN it is used important for the decoder to verify the origin of this key, for example to prevent the decoder communicating information in response to the reception of a public key belonging to a fraudulent user.

To this end, the public key Kpub is encrypted by a private key KeyG unique to the operator and shown at 3051, the certificate containing Kpub thereafter being communicated to and stored in the smart card 3020 at 3052. At the moment of insertion of the card in the decoder, the certificate is decrypted and authenticated by the decoder at 3053 using the equivalent public key KeyG stored at 3054. The value of Kpub thus obtained will thereafter be used for the subsequent encryption steps.

Whilst the data stream described at 3030 and re-encrypted at 3031 has been described in relation to audiovisual data, this may equally correspond to a stream of control word data. As before, in such an embodiment, ECMs containing the control word are decrypted at 3030 and re-encrypted at 3031 for transmission to the decoder. The decrypted control word data obtained at 3033 is then used by the decoder to descramble an associated audiovisual data stream.

#### Encryption of Data Stream at Transmitter

The above embodiments relate to a first type of realisation of the invention in which the encryption of the data stream communicated from the card to the decoder is carried out by the smart card itself. In the following embodiment, an alternative realisation will be described with reference to Figure 5 in which the encryption is carried out further upstream, at the transmitter. As will become clear, this is in addition to the conventional encryption or scrambling of the data stream.

Figure 5 represents the flow of information in this embodiment between the

transmitter 2008, smart card 3020 and decoder 2020. As will be appreciated, whilst this figure shows the information being transmitted directly between transmitter and smart card in order to simplify the explanation, any signals received by the smart card will have of course been received and communicated to the card via the receiver/decoder unit. Similarly, whilst the transmitter has been represented as a single functional block in this case, the encryption of the transmitted message may be carried out by separate elements of the system, as described in relation to Figures 1 and 2.

10 In this embodiment, the audiovisual data stream is encrypted at 3050 by an encryption key  $K_t$ , the exact value of which is dependant on a universal variable  $t$  known to all elements of the system, for example, the real time and/or date of transmission. The encrypted data  $f(\text{DATA})$  is then scrambled as in conventional systems at 3051 by a control word and the resulting encrypted and scrambled data transmitted and  
15 communicated to the security module 3020 within the decoder 2020. The scrambled data is then descrambled at 3020 by the security module.

Unlike existing systems, the data will still be in an encrypted form  $f(\text{DATA})$  and will be passed in this form to the decoder 2020 for decryption at the point 3052. The  
20 decoder 2020 also possesses an equivalent of the key  $K_t$  and, if universally available information such as time and/or date is used, will also be in possession of the value  $t$ . The data may then be decrypted and processed by decoder.

By using a changing universal variant, the system avoids the problem that any  
25 recording of the encrypted control stream  $f(\text{CW})$  obtained by monitoring the card/decoder communications could be used by unauthorised users in the future, since the control stream usable at the moment of transmission will not be usable by a decoder at a future time/date. In contrast, the fact that a universal variable is chosen means that no explicit communication of this variable between the transmitter/decoder  
30 is necessary.

In the above described embodiment, the security module 3020 carries out on-board

-19-

descrambling of the encrypted and scrambled data, using an exploitation key to decrypt a stream of ECM data (not shown) so as to obtain control word data needed for the first descrambling step.

- 5 In an alternative embodiment, the steps shown in Figure 5 may be carried out on the control word data itself, by encrypting at 3051 the once-encrypted control word data using an exploitation key Cex, carrying out a first decryption on the card 3020 using the equivalent exploitation key and thereafter carrying out a second decryption at 3052 using the value t to obtain control word data in clear form. This may then be used
- 10 to descramble associated scrambled audiovisual data received by the decoder.

Whilst less secure than the previous embodiments, this type of system has the advantage that it may be simply implemented in existing systems without any need, for example, to generate new smart cards and the modifications needed to the decoder

15 and transmitter units may be introduced by reprogramming.

As will be understood, all of the embodiments described with reference to Figures 3 to 5 may be implemented separately or in any combination to increase the level of security, if required.

20



CLAIMS

1. A method of transmission and reception of a scrambled data stream in which the  
5 scrambled data stream is transmitted to a decoder and thereafter passed to and  
descrambled by a portable security module inserted in the decoder and characterised  
in that the data stream is passed from the security module to the decoder in an  
encrypted form, to be decrypted and subsequently used by the decoder.
- 10 2. A method as claimed in claim 1, in which the data stream is encrypted in the  
security module by a first encryption key before being passed back to the decoder for  
decryption using an equivalent of the first key.
- 15 3. A method as claimed in claim 2 in which the data stream is encrypted in the  
security module by a first encryption key variable in dependence on a decoder identity  
value, the decoder possessing an equivalent of the key and value necessary to decrypt  
the data stream.
- 20 4. A method as claimed in claim 3 in which the decoder identity value is encrypted  
by a personalised key known to the security module and transmitter, the decoder  
identity value being transmitted in an encrypted form to the decoder for  
communication to the security module.
- 25 5. A method as claimed in 3 in which the decoder identity value is encrypted by a  
personalised key known to the security module, the encrypted decoder identity value  
being stored in the decoder during manufacture for communication to the security  
module upon insertion of the security module in the decoder.
- 30 6. A method as claimed in claim 2 in which the data stream is encrypted in the  
security module by a first encryption key dependant on a random or pseudo-random  
number.

7. A method as claimed in claim 6, in which the random number is communicated between the decoder and security module encrypted by a second encryption key.
8. A method as claimed in claim 7, in which the random number is generated and encrypted by the second encryption key in the security module and communicated to the decoder for decryption by an equivalent of the second key stored in the decoder.
9. A method as claimed in claim 7 in which the random number is generated and encrypted by the second encryption key at the decoder and communicated to the security module for decryption by an equivalent of the second key stored in the security module.
10. A method as claimed in claim 9 in which the second key used to encrypt the random number in the decoder corresponds to a public key, the security module being provided with the equivalent private key necessary to decrypt the random number value.
11. A method as claimed in claim 9 or 10 in which at least the second key held by the security module is unique to that security module.
12. A method as claimed in any of claims 7 to 11, in which the second key held by the decoder is encrypted by a third key before communication to the decoder, the decoder possessing the corresponding third key so as to hereby decrypt and verify the second decoder key.
13. A method as claimed in claim 12, in which the third key used to encrypt the second decoder key is a private key, the decoder possessing the equivalent public key to decrypt and verify the communicated second key.
14. A method as claimed in claim 1 in which the data stream is encrypted at the point of transmission by a first encryption key and decrypted by the decoder by an equivalent of this key.



15. A method as claimed in claim 14 in which the data stream is encrypted at the point of transmission by a first encryption key dependant on a variable known to both the transmitter and the decoder and decrypted at the decoder by an equivalent of this key and variable.
- 5
16. A method as claimed in claim 15 in which the variable corresponds to the real time and/or date of transmission.
17. A method as claimed in any of claims 14 to 16 in which the first encrypted data stream is further scrambled at the point of transmission, descrambled in the security module and then passed in its first encrypted form to the decoder.
- 10
18. A method of transmission and reception of scrambled data combining a method of encryption of the data stream in the card as claimed in any of claims 2 to 13, separately or in combination, together with a method of encryption of the control word at the point of transmission, as claimed in any of claims 14 to 17.
- 15
19. A method as claimed in any of claims 1 to 18 in which the data stream passed in encrypted form between the security module and decoder comprises audiovisual data.
- 20
20. A method as claimed in any of claims 1 to 18 in which the data stream passed in encrypted form between the security module and decoder comprises a control word stream, the control word stream once decrypted by the decoder being thereafter used by the decoder to descramble associate scrambled audiovisual data.
- 25
21. A method as claimed in any preceding claim in which the scrambled data stream is transmitted as part of a television broadcast.
22. A decoder and portable security module adapted for use in a method as claimed in any preceding claim.
- 30

-23-

23. A method of transmission and reception of a scrambled data stream substantially as herein described.

Fig.1.

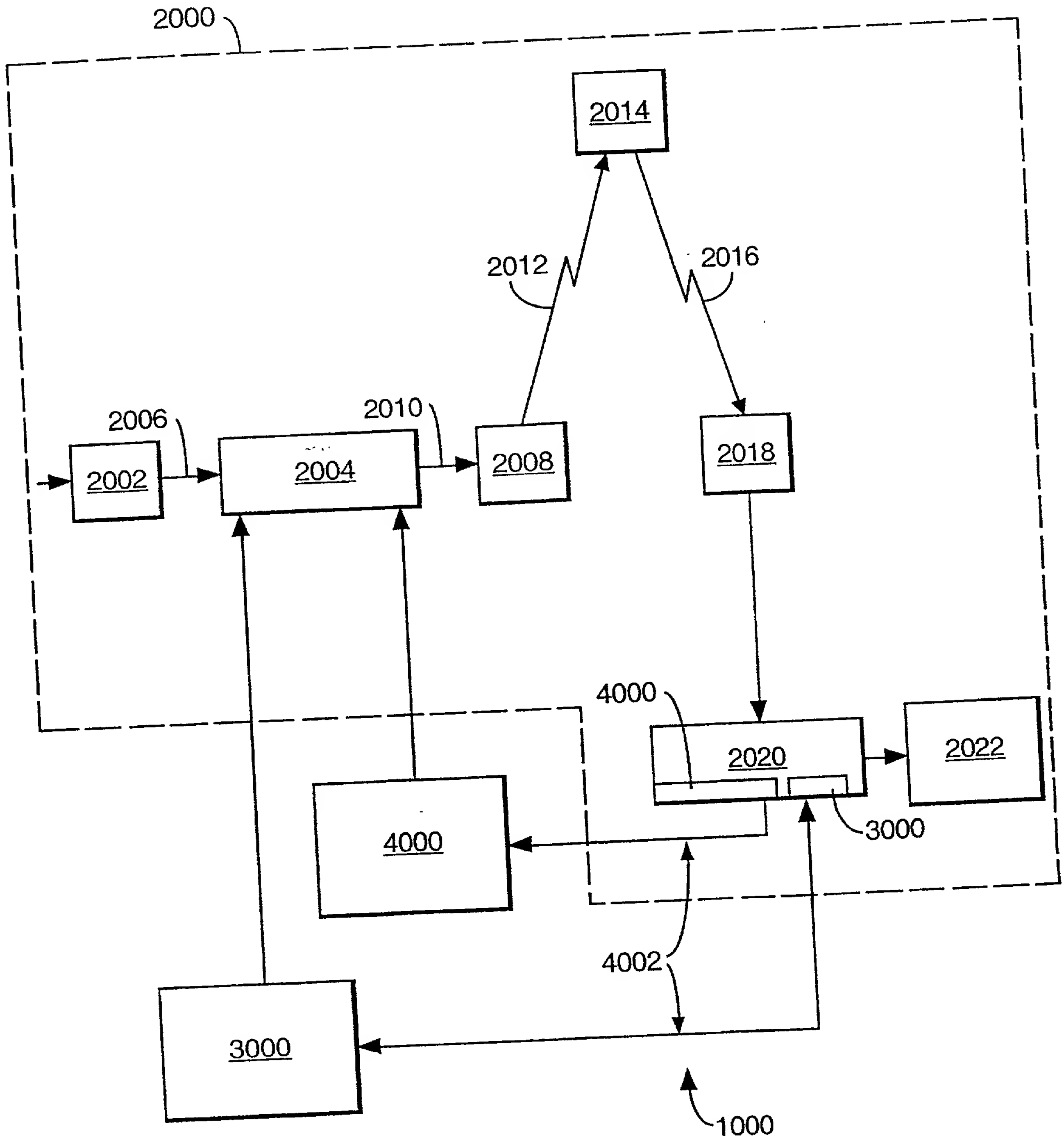


Fig.2.

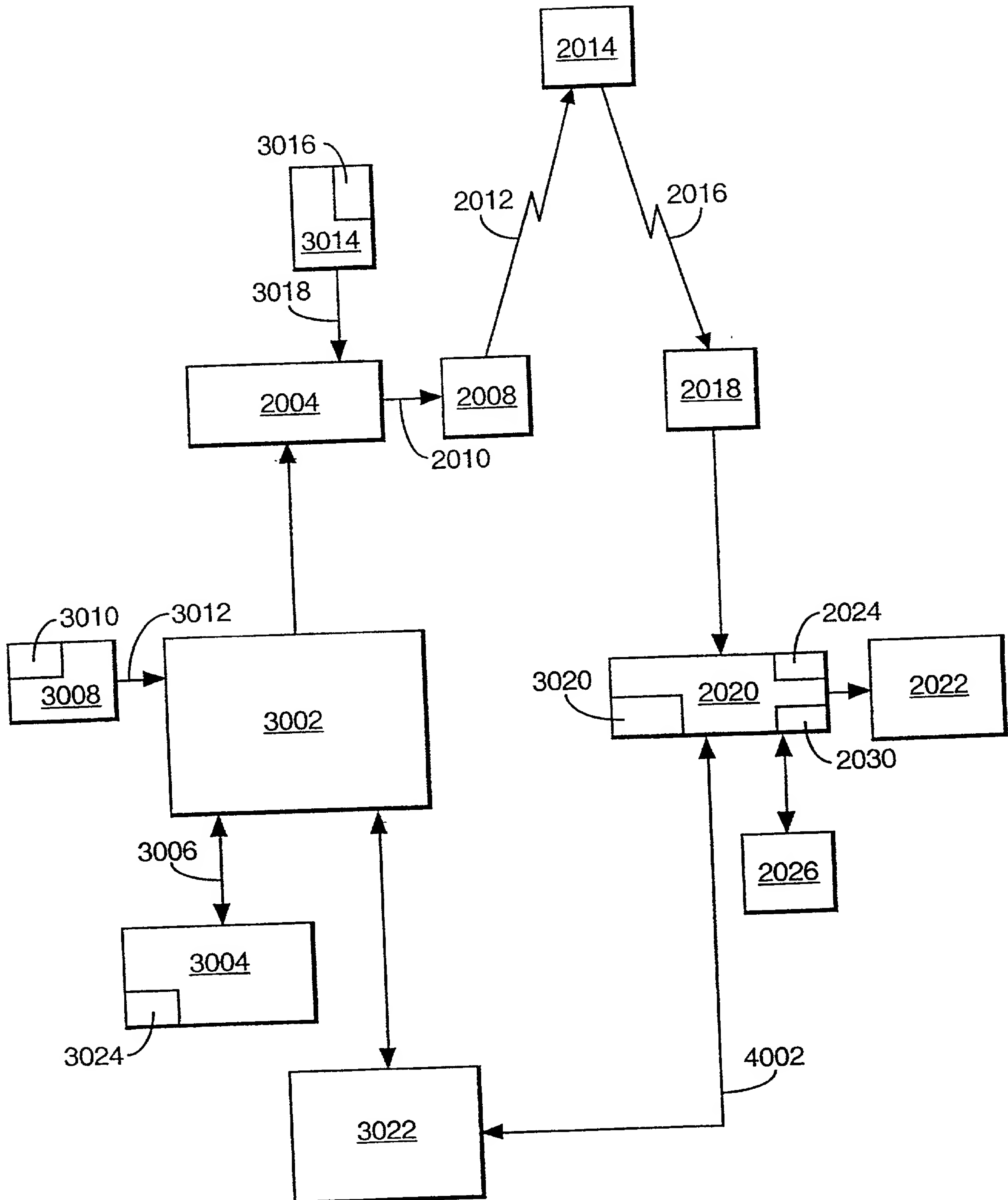


Fig.3.

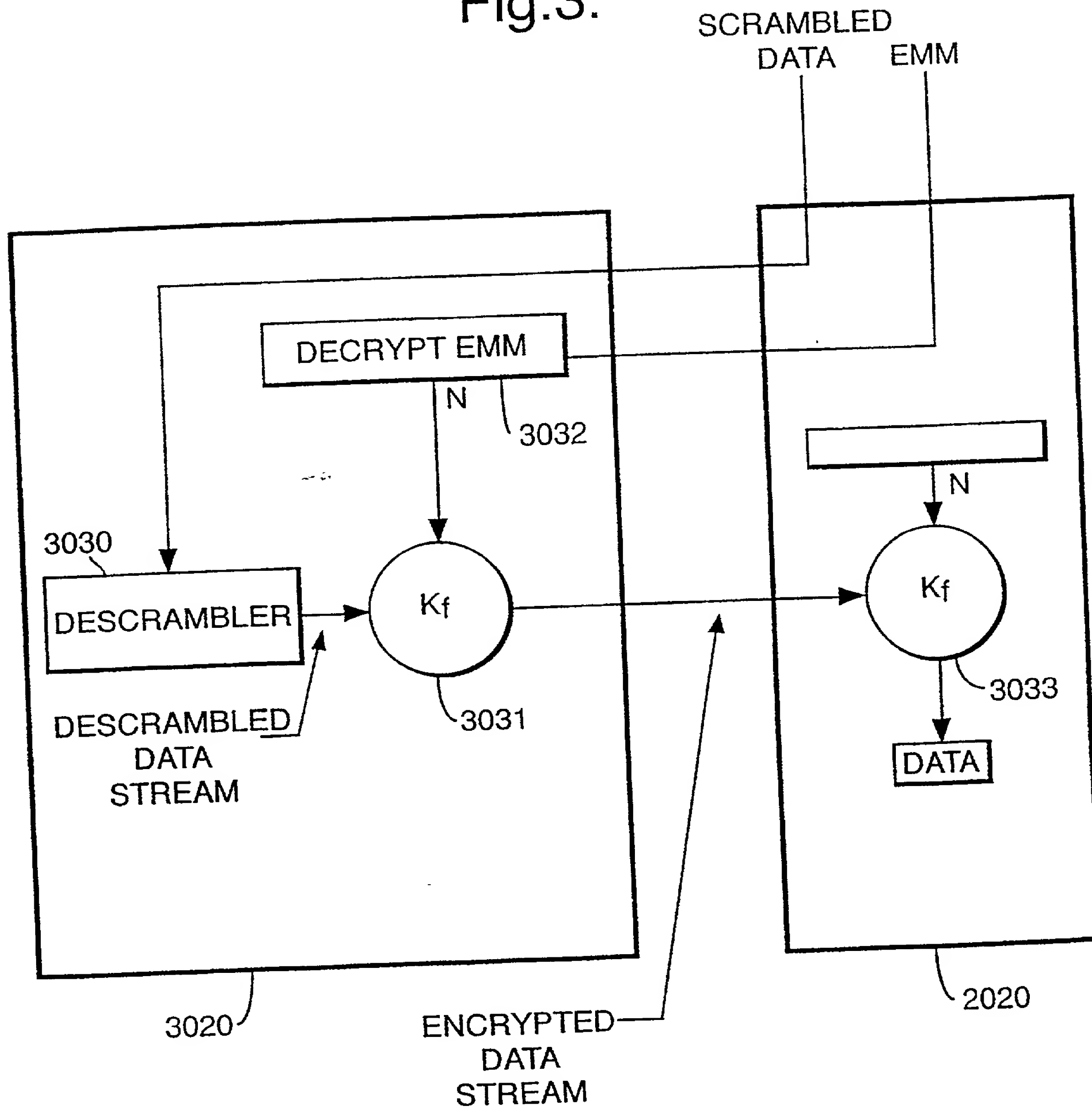


Fig. 4

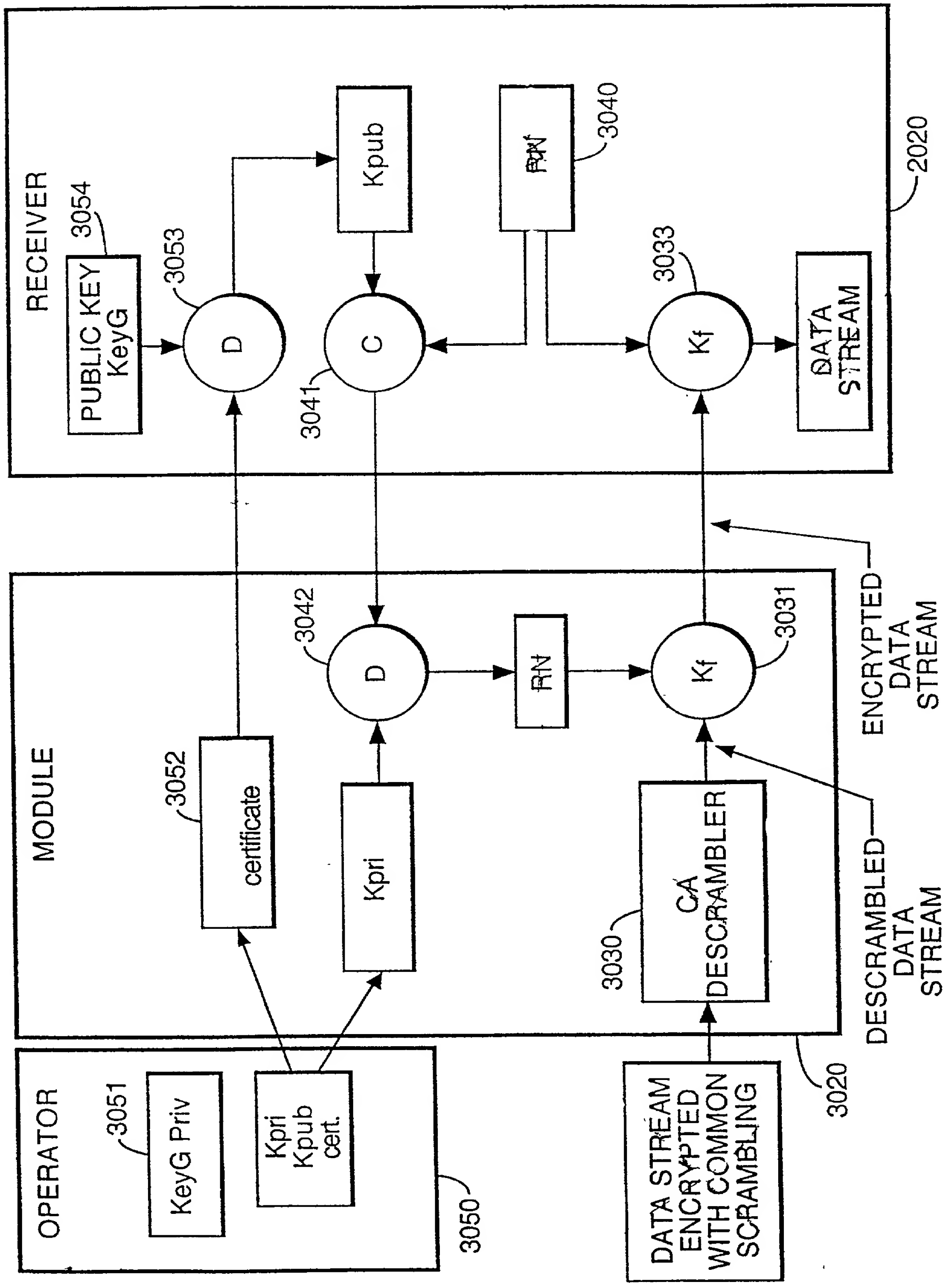
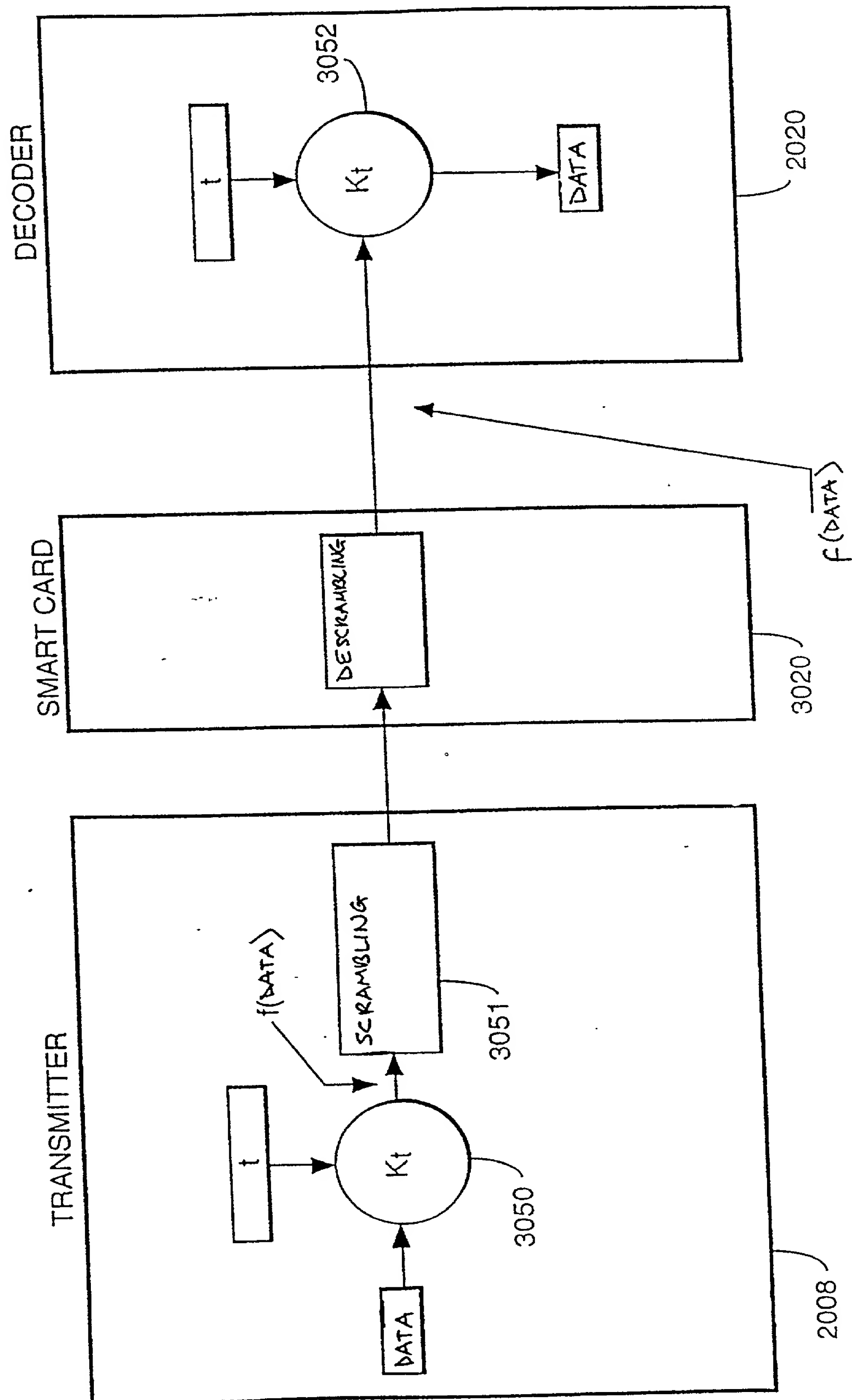


Fig. 5.



**Declaration and Power of Attorney for Patent Application****Déclaration et Pouvoirs pour Demande de Brevet****French Language Declaration****22511**

PATENT TRADEMARK OFFICE

PTO  
09/53/071  
03/28/00

En tant que l'inventeur nommé ci-après, je déclare par le présent acte que:

Mon domicile, mon adresse postale et ma nationalité sont ceux figurant ci-dessous à côté de mon nom.

Je crois être le premier inventeur original et unique (si un seul nom est mentionné ci-dessous), ou l'un des premiers co-inventeurs originaux (si plusieurs noms sont mentionnés ci-dessous) de l'objet revendiqué, pour lequel une demande de brevet a été déposée concernant l'invention intitulée

\_\_\_\_\_

\_\_\_\_\_

et dont la description est fournie ci-joint à moins que la case suivante n'ait été cochée:

- ☐ a été déposée le \_\_\_\_\_  
sous le numéro de demande des Etats-Unis ou le  
numéro de demande international PCT  
\_\_\_\_\_ et modifiée le  
\_\_\_\_\_ (le cas échéant).

Je déclare par le présent acte avoir passé en revue et compris le contenu de la description ci-dessus, revendications comprises, telles que modifiées par toute modification dont il aura été fait référence ci-dessus.

Je reconnais devoir divulguer toute information pertinente à la brevetabilité, comme défini dans le Titre 37, § 1.56 du Code fédéral des réglementations.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Method and Apparatus for Encrypted

Data Stream Transmission

the specification of which is attached hereto unless the following box is checked:

- ☐ was filed on \_\_\_\_\_  
as United States Application Number or PCT  
International Application Number  
\_\_\_\_\_ and was amended on  
\_\_\_\_\_ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.



**French Language Declaration**

Je revendique par le présent acte avoir la priorité étrangère, en vertu du Titre 35, § 119(a)-(d) ou § 365(b) du Code des Etats-Unis, sur toute demande étrangère de brevet ou certificat d'inventeur ou, en vertu du Titre 35, § 365(a) du même Code, sur toute demande internationale PCT désignant au moins un pays autre que les Etats-Unis et figurant ci-dessous et, en cochant la case, j'ai aussi indiqué ci-dessous toute demande étrangère de brevet, tout certificat d'inventeur ou toute demande internationale PCT ayant une date de dépôt précédant celle de la demande à propos de laquelle une priorité est revendiquée.

Prior foreign application(s)  
Demande(s) de brevet antérieure(s)

<u>97402322.8</u>	<u>Europe</u>
(Number)	(Country)
(Numéro)	(Pays)
<u>98401388.8</u>	<u>Europe</u>
(Number)	(Country)
(Numéro)	(Pays)

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, § 119(e) du Code des Etats-Unis, de toute demande de brevet provisoire effectuée aux Etats-Unis et figurant ci-dessous.

<u>(Application No.)</u>	<u>(Filing Date)</u>
<u>(N° de demande)</u>	<u>(Date de dépôt)</u>

<u>(Application No.)</u>	<u>(Filing Date)</u>
<u>(N° de demande)</u>	<u>(Date de dépôt)</u>

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, § 120 du Code des Etats-Unis, de toute demande de brevet effectuée aux Etats-Unis, ou en vertu du Titre 35, § 365(c) du même Code, de toute demande internationale PCT désignant les Etats-Unis et figurant ci-dessous et, dans la mesure où l'objet de chacune des revendications de cette demande de brevet n'est pas divulgué dans la demande antérieure américaine ou internationale PCT, en vertu des dispositions du premier paragraphe du Titre 35, § 112 du Code des Etats-Unis, je reconnais devoir divulguer toute information pertinente à la brevetabilité, comme défini dans le Titre 37, § 1.56 du Code fédéral des réglementations, dont j'ai pu disposer entre la date de dépôt de la demande antérieure et la date de dépôt de la demande nationale ou internationale PCT de la présente demande:

<u>WO 99/18729</u>	<u>PCT</u>	<u>(02.10.1998)</u>
--------------------	------------	---------------------

<u>(Application No.)</u>	<u>(Filing Date)</u>
<u>(N° de demande)</u>	<u>(Date de dépôt)</u>

<u>(Application No.)</u>	<u>(Filing Date)</u>
<u>(N° de demande)</u>	<u>(Date de dépôt)</u>

Je déclare par le présent acte que toute déclaration ci-incluse est, à ma connaissance, véridique et que toute déclaration formulée à partir de renseignements ou de suppositions est tenue pour véridique; et de plus, que toutes ces déclarations ont été formulées en sachant que toute fausse déclaration volontaire ou son équivalent est passible d'une amende ou d'une incarcération, ou des deux, en vertu de la Section 1001 du Titre 18 du Code des Etats-Unis, et que de telles déclarations volontairement fausses risquent de compromettre la validité de la demande de brevet ou du brevet délivré à partir de celle-ci.

I hereby claim foreign priority under Title 35, United States Code, § 119(a)-(d) or § 365 (b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below, and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

	Priority Claimed <u>Droit de priorité revendiqué</u>
--	---

02 October 1997

(Day/Month/Year Filed)  
(Jour/Mois/Année de dépôt)

☒

09 June 1998  
(Day/Month/Year Filed)  
(Jour/Mois/Année de dépôt)

☒

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below.

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

Pending

<u>(Status) (patented, pending, abandoned)</u>
<u>(Statut) (breveté, en cours d'examen, abandonné)</u>

<u>(Status) (patented, pending, abandoned)</u>
<u>(Statut) (breveté, en cours d'examen, abandonné)</u>

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**French Language Declaration**

Je revendique par le présent acte avoir la priorité étrangère, en vertu du Titre 35, § 119(a)-(d) ou § 365(b) du Code des Etats-Unis, sur toute demande étrangère de brevet ou certificat d'inventeur ou, en vertu du Titre 35, § 365(a) du même Code, sur toute demande internationale PCT désignant au moins un pays autre que les Etats-Unis et figurant ci-dessous et, en cochant la case, j'ai aussi indiqué ci-dessous toute demande étrangère de brevet, tout certificat d'inventeur ou toute demande internationale PCT ayant une date de dépôt précédant celle de la demande à propos de laquelle une priorité est revendiquée.

Prior foreign application(s)

Demande(s) de brevet antérieure(s)

98401389.6 Europe

(Number) (Country)

(Numéro) (Pays)

(Number) (Country)

(Numéro) (Pays)

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, § 119(e) du Code des Etats-Unis, de toute demande de brevet provisoire effectuée aux Etats-Unis et figurant ci-dessous.

(Application No.) (Filing Date)  
(N° de demande) (Date de dépôt)

(Application No.) (Filing Date)  
(N° de demande) (Date de dépôt)

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, § 120 du Code des Etats-Unis, de toute demande de brevet effectuée aux Etats-Unis, ou en vertu du Titre 35, § 365(c) du même Code, de toute demande internationale PCT désignant les Etats-Unis et figurant ci-dessous et, dans la mesure où l'objet de chacune des revendications de cette demande de brevet n'est pas divulgué dans la demande antérieure américaine ou internationale PCT, en vertu des dispositions du premier paragraphe du Titre 35, § 112 du Code des Etats-Unis, je reconnais devoir divulguer toute information pertinente à la brevetabilité, comme défini dans le Titre 37, § 1.56 du Code fédéral des réglementations, dont j'ai pu disposer entre la date de dépôt de la demande antérieure et la date de dépôt de la demande nationale ou internationale PCT de la présente demande:

(Application No.) (Filing Date)  
(N° de demande) (Date de dépôt)

(Application No.) (Filing Date)  
(N° de demande) (Date de dépôt)

Je déclare par le présent acte que toute déclaration ci-incluse est, à ma connaissance, véridique et que toute déclaration formulée à partir de renseignements ou de suppositions est tenue pour véridique; et de plus, que toutes ces déclarations ont été formulées en sachant que toute fausse déclaration volontaire ou son équivalent est passible d'une amende ou d'une incarcération, ou des deux, en vertu de la Section 1001 du Titre 18 du Code des Etats-Unis, et que de telles déclarations volontairement fausses risquent de compromettre la validité de la demande de brevet ou du brevet délivré à partir de celle-ci.

I hereby claim foreign priority under Title 35, United States Code, § 119(a)-(d) or § 365 (b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below, and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Priority Claimed  
Droit de priorité revendiqué

09 June 1998

(Day/Month/Year Filed)  
(Jour/Mois/Année de dépôt)

☒☐

(Day/Month/Year Filed)  
(Jour/Mois/Année de dépôt)

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below.

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

(Status) (patented, pending, abandoned)  
(Statut) (breveté, en cours d'examen, abandonné)

(Status) (patented, pending, abandoned)  
(Statut) (breveté, en cours d'examen, abandonné)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**French Language Declaration**

POUVOIRS: En tant que l'inventeur cité, je désigne par la présente l'(les) avocat(s) et/ou agent(s) suivant(s) pour qu'ils poursuive(nt) la procédure de cette demande de brevet et traite(nt) toute affaire s'y rapportant avec l'Office des brevets et des marques: (mentionner le nom et le numéro d'enregistrement).

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: (list name and registration number)

Jonathan P. Osha, Reg. No. 33,986, Alan D. Rosenthal, Reg. No. 27,833, Richard A. Fagin, Reg. No. 39,182, Adenike Adewuya, Reg. No. 42,254, David E. Mixon, Reg. No. 43,809, Thomas K. Scherer, Reg. No. 45,079, K. KaRan Reed, Reg. No. 45,036; Jeffrey S. Bergman, Reg. No. P45,925, Scott W. Hejny, Reg. No. P45,882, W. Thomas Morrow, Reg. No. P45,953, Y. Renee Alsandor, Reg. No. P45,883


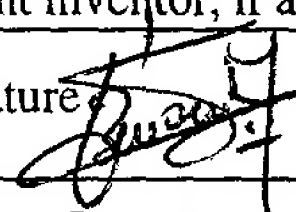
Adresser toute correspondance à:

Send Correspondence to: **Jonathan P. Osha**  
**ROSENTHAL & OSHA L.L.P.**  
 700 Louisiana, Suite 4550  
 Houston, Texas 77002

Adresser tout appel téléphonique à:  
 (nom et numéro de téléphone)

Direct Telephone Calls to:  
 (name and telephone number)

**Jonathan P. Osha (713) 228-8600**

Nom complet de l'unique ou premier inventeur	Full name of sole or first inventor <b>Michel MAILLARD</b>
Signature de l'inventeur                      Date	Inventor's signature  Date <b>15/03/2000</b>
Domicile	Residence <b>13 avenue du Parc</b> <b>78120 Rambouillet, FRANCE</b>
Nationalité	Citizenship
Adresse postale	Post Office Address <b>13 avenue du Parc</b> <b>78120 Rambouillet, FRANCE</b>
Nom complet du second co-inventeur, le cas échéant	Full name of second joint inventor, if any <b>Christian BENARDEAU</b>
Signature du second inventeur                      Date	Second Inventor's signature  Date <b>15/03/00</b>
Domicile	Residence <b>13, allée des Puisatiers</b> <b>F-77600 Bussy-Saint-Georges, FRANCE</b>
Nationalité	Citizenship
Adresse postale	Post Office Address <b>13, allée des Puisatiers</b> <b>F-77600 Bussy-Saint-Georges, FRANCE</b>

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)

# **French Language Declaration**

POUVOIRS: En tant que l'inventeur cité, je désigne par la présente l'(les) avocat(s) et/ou agent(s) suivant(s) pour qu'ils poursuive(nt) la procédure de cette demande de brevet et traite(nt) toute affaire s'y rapportant avec l'Office des brevets et des marques. (mentionner le nom et le numéro d'enregistrement).

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: (list name and registration number)

Jonathan P. Osha, Reg. No. 33,986, Alan D. Rosenthal, Reg. No. 27,833, Richard A. Fagin, Reg. No. 39,182, Adenike Adewuya, Reg. No. 42,254; David E. Mixon, Reg. No. 43,809, Thomas K. Scherer, Reg. No. 45,079, K. KaRan Reed, Reg. No. 45,036, Jeffrey S. Bergman, Reg. No. P45,925, Scott W. Hejny, Reg. No. P45,882, W. Thomas Morrow, Reg. No. P45,953, Y. Renee Alsandor, Reg. No. P45,883

Adresser toute correspondance à:

Send Correspondence to: **Jonathan P. Osha**  
**ROSENTHAL & OSHA L.L.P.**  
700 Louisiana, Suite 4550  
Houston, Texas 77002

Adresser tout appel téléphonique à:  
(nom et numéro de téléphone)

Direct Telephone Calls to:  
(name and telephone number)  
**Jonathan P. Osha (713) 228-8600**

Nom complet de l'unique ou premier inventeur	Jean-Luc DAUVOIS Full name of third inventor, if any		
Signature de l'inventeur	Date	Inventor's signature	Date 16/03/2000
Domicile	Residence 19, rue Eugene-Manuel F-75116 Paris, FRANCE		
Nationalité	Citizenship		
Adresse postale	Post Office Address 19, rue Eugene-Manuel F-75116 Paris, FRANCE		
Nom complet du second co-inventeur, le cas échéant	Full name of fourth inventor, if any		
Signature du second inventeur	Date	Fourth Inventor's signature	Date
Domicile	Residence		
Nationalité	Citizenship		
Adresse postale	Post Office Address		

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)